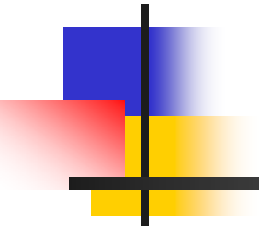
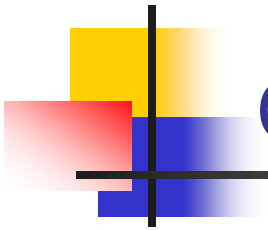


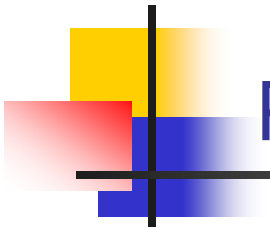
BAN LOGIC

This note is manily is taken from Internet with unknown trace of source and is further enhanced



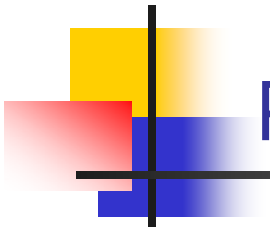
Outline

- Introduction
- Basic Notations
- Formalism & Rules
- Goals of Authentication
- Step in Protocol Analysis
- Needham-Schroeder Protocol
- Kerberos
- Flaw/Advantages of BAN Logic
- Conclusion



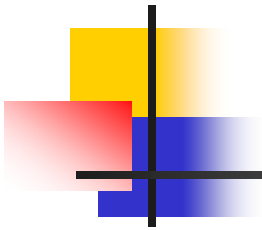
Formal Verification of Cryptographic Protocols

- *Expert system based approaches*
  - Knowledge of human experts is formalized into deductive rules that can be used by a protocol designer to investigate different scenarios
  - Main drawback: not well suited to find flaws in cryptographic protocols that are based on unknown attacking techniques
- *Algebraic approaches:*
  - Cryptographic protocols are specified as algebraic systems
  - Analysis is conducted by examining algebraic term-rewriting properties of the model and inspecting if the model can attain certain desirable or undesirable states
- *Specific logic based approaches:*
  - Approaches of this class define a set of predicates and a mapping of messages exchanged during a protocol run into to a set of formula
  - A generic set of rules allows then to analyze the *knowledge* and *belief* that is obtained by the peer entities of a cryptographic protocol during a protocol run (BAN logics)



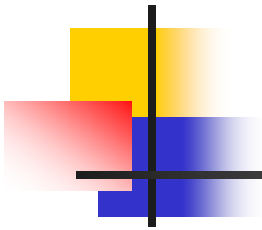
Problems with the design of the protocols

- Lack of assumptions
- Lack of formal descriptions
- Lack of clarity



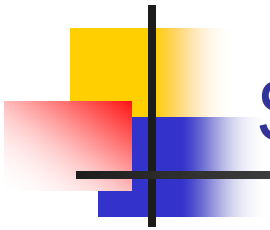
BAN Logic

- BAN Logic was formulated by Burrows, Abadi, and Needham in1989
- BAN Logic is based on an agreed set of deduction rules for formally reasoning about the authentication protocols and is often referred to as a logic of authentication.
- It is a formal method for verifying that two principals (people, computer, services) are entitled to believe they are communicating with each other and not the intruders.
- BAN Logic is based on belief system
  - on the beliefs of trustworthy parties involved in the protocol and the evolution of these beliefs through communication processes



Purpose of BAN Logic

- BAN logic helps to prove whether or not a protocol does or does not meet its security goals.
- BAN logic helps make the protocols more efficient by eliminating messages, contents of message, or encryptions of messages. Despite eliminating them, the security goals still can be reached.
- BAN logic helps clarify the protocol's assumptions by formally stating them.



Steps of BAN Logic

(1) The protocol is first transformed into some “idealized” form

(2) Identify the initial assumptions in the language of BAN logic

(3) Use the postulates and rules of the logic to deduce new predicates

(4) Interpret the statements have proved by the process? Have the goals met?

Basic Notations

- Formalism built on several objects: principals, encryption keys, and formulas(statements)
- A, B and S denote specific principals (people, computers, services)
- $K_{ab,}$ $K_{as,}$ and K_{bs} denote specific shared keys
- $K_{b,}$ $K_{a,}$ and K_{s} denote specific public keys
- K_{b}^{-1}, K_{a}^{-1}, and K_{s}^{-1} denote corresponding secret keys
- $N_{a,}$ $N_{b,}$ N_{c} denote specific statements
- P, Q, and R be principals
- X and Y be statements
- K denotes keys

Notations

P |≡X: P *believes* X. P would be entitled to believe X. The principal P may act as though X is true.

P ◁ X: P *sees* X. P can read the contents of X (possibly after decryption, assuming P has the needed keys) and P can include X in messages to other principals.

P |~ X: P *once said* X: P at some time sent a message including the statement X. It is not known when the message was sent (in the past or in the current run of the protocol) but P believed that X was true when it send the message.

P |⇒ X: P controls X. P has jurisdiction over X. P is a trusted authority on the truth of X.

#(X): X is *fresh*. Using the logic, time is divided into two *epoch*, the past and the present. The present begins with the start of the current execution of the current protocol. X is fresh if it is not contained in any message sent in the past.

Notations

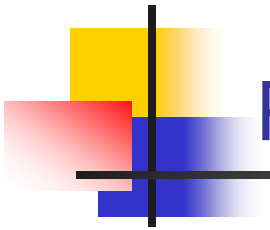
$\overset{K}{\leftrightarrow}$ **P Q:** K is a shared key for P and Q. K is a secure key for communication between P and Q, and it will never be discovered by any principal except for P or Q, or a principal trusted by either P or Q.

$\overset{K}{\mapsto}$ **P:** K is a *public key* for P. The matching secret key(the inverse of K, denoted by K^{-1} will never be discovered by any principal except P, or a principals trusted by P.

$\{X\}_K$**:** X *encrypted under* K. It represents the message X encrypted using the key K.

Notations

- **P** $|\equiv$ **X** : **P** believes **X**
- **P** $\triangleleft$ **X** : **P** sees **X**
- **P** $|\sim$ **X** : **P** once said **X**
- # (**X**) : **X** is fresh
- **P** $|\Rightarrow$ **X** : **P** control over **X**
- **{X}k** : X is encrypted under k
- $P \overset{k}{\leftrightarrow} Q$: **K** is a good key for communication between **P** and **Q**
- $\overset{k}{\mapsto} P$: **P** has **K** as a public key
- $\overset{k^{-1}}{\mapsto} P$: **P** knows a private key



Formalism

Inference Rules

- More information about the meaning of logical constructions can be deduced from a collection of inference rules
- These rules help generate a set of beliefs to provide soundness to the protocol
- Messages can't be deduced by those without the proper keys
- "," means conjunction which is used to append or combine something and _____ means implies

Rules (Cont'd)

- To express that a statement Z follows from a conjunction of statements X and Y

$$\frac{(X, Y)}{Z}$$

- **Message meaning rule (MMR):** Rule concerns the interpretation of messages. This rule helps to explain the origin of the messages For shared keys, if $P \neq Q$,

$$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P,\ P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

Rules (Cont'd)

- **Nonce-verification rule (NVR):** This rule checks that a message is recent, and also checks if the sender still believes in it.

$$\frac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

- **Jurisdiction rule (JR):** This rule states what it means for a principal to be the trusted authority on the truth of X

$$\frac{P \mid\equiv Q \mid\Rightarrow X,\ \ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

Rules (Cont'd)

- **Belief Rule (BR):** The rule states that a principal believes a collection of statements if and only if it believes each of the statements individually.

A) $$\frac{P \mid\equiv X,\ P \mid\equiv Y}{P \mid\equiv (X, Y)}$$

B) $$\frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

C) $$\frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$$

Rules (Cont'd)

- **Seeing rule (SR):** This rule says that a principal sees all the components of every message it sees, provided that the principal knows the necessary key.

A) $$\frac{P \lhd (X, Y)}{P \lhd X}$$

B) $$\frac{P \mid\equiv \; Q \overset{K}{\leftrightarrow} P, \; P \lhd \{X\}_K}{P \lhd X}$$

- **Freshness Rule (FR):** This rule states that any message with a fresh component is also fresh

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$$

Rules

(MMR):

$$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P,\ P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

(BR):

$$\frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

(NVR):

$$\frac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

(SR):

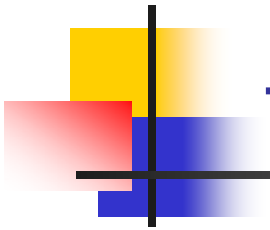
$$\frac{P \mid\equiv \overset{K}{Q \leftrightarrow P},\ P \triangleleft \{X\}_K}{P \triangleleft X}$$

(JR):

$$\frac{P \mid\equiv Q \mid\Rightarrow X,\ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

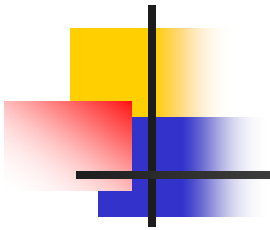
(FR):

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$$



The role of Time in BAN logic

- The logic has no notion of time to be associated with individual statements
- Explicit use of time in the logic is avoided
- Division of time into 2 epochs: **past** and **present**
- Timestamps are used in some authentication protocols but timestamps are not required to be made explicit in the logic, only freshness is required, so past and present are sufficient time divisions



The Role of Time in BAN Logic (Cont'd)

Present

- Begins at the start of the run of the protocol
- Beliefs hold through the entirety of protocol run

Past

- Beliefs not carried forward into the present
- All messages sent before the present considered part of past.

Idealized Protocols

- Typically, each protocol step as:

  P → Q : *message*

- **What does this denote?**

  Principal P sends the message and that principal Q receives the message. It is an *informal* notation

- **What is wrong with it?**

  Often ambiguous, obscure in meaning, not appropriate for formal analysis

- **How to fix it?**

  Transform each protocol into an idealized form

- Steps

  1) Omit the parts of the message that do not contribute to the beliefs of the recipient

  2) Omit clear text communication because it can be forged

Idealized Protocols (Cont'd)

Example:
What we normally see in literature:

$$A \rightarrow B : \{A, K_{ab}\}K_{bs}$$

Idealized version:

$$A \rightarrow B : \{A \overset{Kab}{\leftrightarrow} B\}K_{bs}$$

When message is sent to B it can be deduced that:

$$B \triangleleft \{A \overset{Kab}{\leftrightarrow} B\}k_{bs}$$

The receiving principle becomes aware of the message (sees the message) and can act upon it.

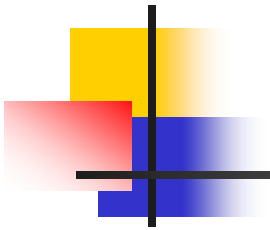
Goals of Authentication

- Authentication rests on communication protected by shared session key, so the goals of authentication may be reached between A and B if there is a K such that:

$$A \overset{K}{\mid\equiv} A \leftrightarrow B \qquad\qquad B \overset{K}{\mid\equiv} A \leftrightarrow B$$

- Some authentication protocols achieve this final goal:

$$A \overset{K}{\mid\equiv} B \mid\equiv A \leftrightarrow B \qquad\qquad B \overset{K}{\mid\equiv} A \mid\equiv A \leftrightarrow B$$



Steps in Protocol Analysis

- Derive the **idealized protocol** from the original one
- Write **assumptions** about the initial state
- Use the **postulates and rules** of the logic to deduce new predicates
- This is **repeated** through all the protocol messages
- Determine if **goals** of authentication have been met

Needham-Schroeder Protocol with Shared Key (NSSK)

Original version without idealization

Message 1 $A \rightarrow S$: A, B, N_a

Message 2 $S \rightarrow A$: $\{N_a, B, K_{ab}, \{K_{ab}, A\}K_{bs}\} K_{as}$

Message 3 $A \rightarrow B$: $\{K_{ab}, A\}K_{bs}$

Message 4 $B \rightarrow A$: $\{N_b\}K_{ab}$

Message 5 $A \rightarrow B$: $\{N_b - 1\}K_{ab}$

NSSK (Cont'd)

Corresponding idealized protocol is as follows:

Message 2 $S \rightarrow A$: $\{N_a, \overset{Kab}{(A \leftrightarrow B)}, \#\overset{Kab}{(A \leftrightarrow B)}, \{\overset{Kab}{A \leftrightarrow B}\}K_{bs}\}\ K_{as}$

Message 3 $A \rightarrow B$: $\{\overset{Kab}{A \leftrightarrow B}\}K_{bs}$

Message 4 $B \rightarrow A$: $\{N_b, \overset{Kab}{(A \leftrightarrow B)}\}K_{ab}$ from B

Message 5 $A \rightarrow B$: $\{N_b, \overset{Kab}{(A \leftrightarrow B)}\}K_{ab}$ from A

NSSK (Cont'd)

- The goal of this idealization is to see if both principals A & B can be convinced of each other's presence.

$$A \overset{K}{|\equiv} A \leftrightarrow B \qquad B \overset{K}{|\equiv} A \leftrightarrow B$$

and

$$A \overset{K}{|\equiv} B |\equiv A \leftrightarrow B \qquad B \overset{K}{|\equiv} A |\equiv A \leftrightarrow B$$

NSSK (Cont'd)

Initial assumptions:

$$A \mid\equiv A \overset{Kas}{\leftrightarrow} S \qquad B \mid\equiv B \overset{Kbs}{\leftrightarrow} S$$

$$S \mid\equiv A \overset{Kas}{\leftrightarrow} S \qquad S \mid\equiv B \overset{Kbs}{\leftrightarrow} S$$

$$S \mid\equiv A \overset{Kab}{\leftrightarrow} B$$

$$A \mid\equiv (S \mid\Rightarrow A \overset{Kab}{\leftrightarrow} B) \qquad B \mid\equiv (S \mid\Rightarrow A \overset{Kab}{\leftrightarrow} B)$$

$$A \mid\equiv (S \mid\Rightarrow \#(A \overset{Kab}{\leftrightarrow} B))$$

NSSK (Cont'd)

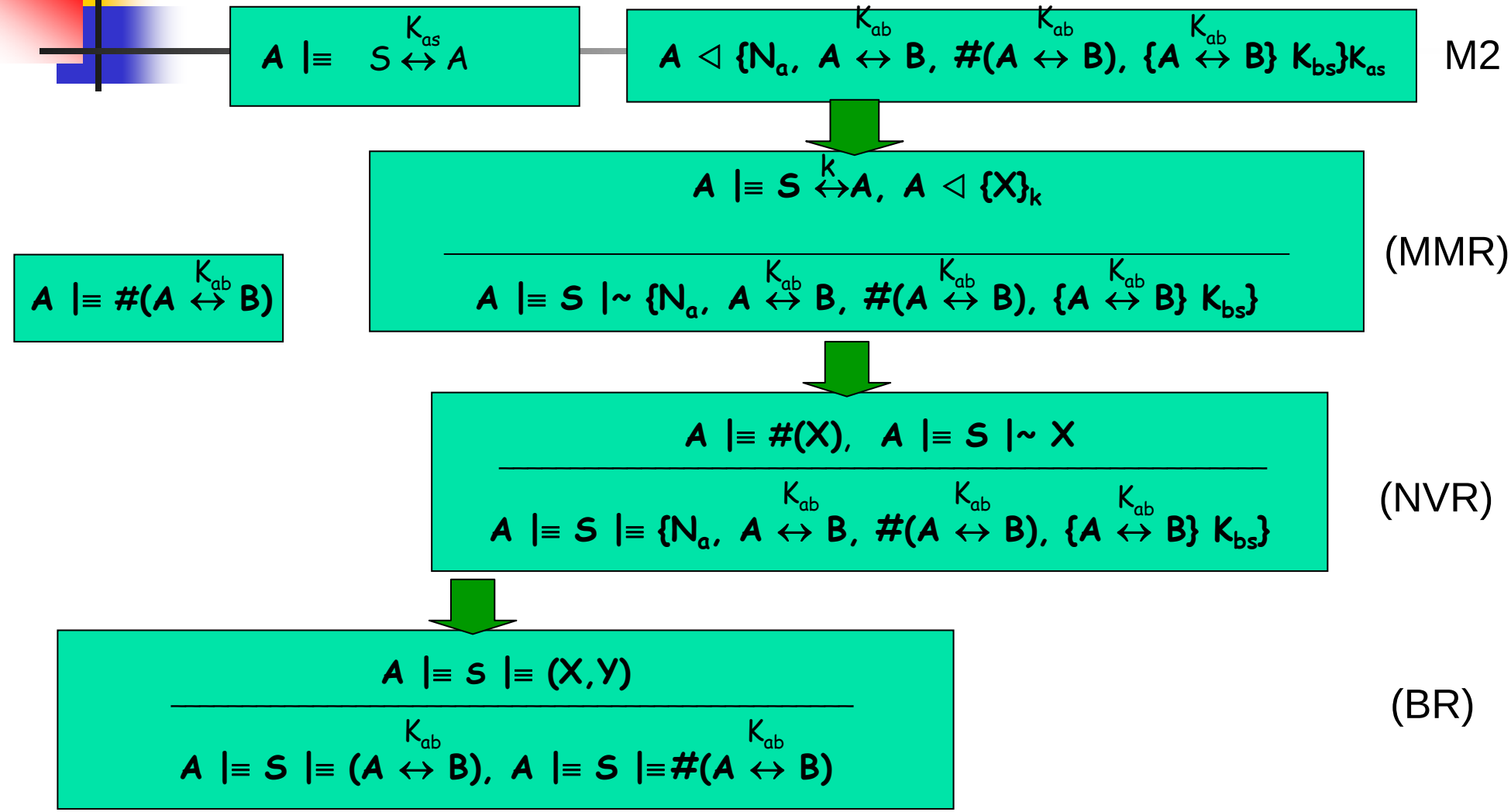
More assumptions (continued)

$$\mathbf{A} \mid\equiv \#(N_a) \qquad \mathbf{B} \mid\equiv \#(N_b)$$

$$\mathbf{S} \mid\equiv \#(A \overset{Kab}{\leftrightarrow} B) \qquad \mathbf{B} \mid\equiv \#(A \overset{Kab}{\leftrightarrow} B)$$

NOTE: The assumption $B \mid\equiv \#(A \overset{Kab}{\leftrightarrow} B)$ meaning B believes in the freshness on the key is an assumption that the authors of the Needham-Schroeder protocol did not realize they were making.

NSSK Verification I



NSSK Verification (Cont'd)

$$A \mid\equiv S \mid\equiv (A \overset{K_{ab}}{\leftrightarrow} B),\ A \mid\equiv S \mid\equiv \#(A \overset{K_{ab}}{\leftrightarrow} B)$$

$$A \mid\equiv (S \mid\Rightarrow A \overset{K_{ab}}{\leftrightarrow} B)$$

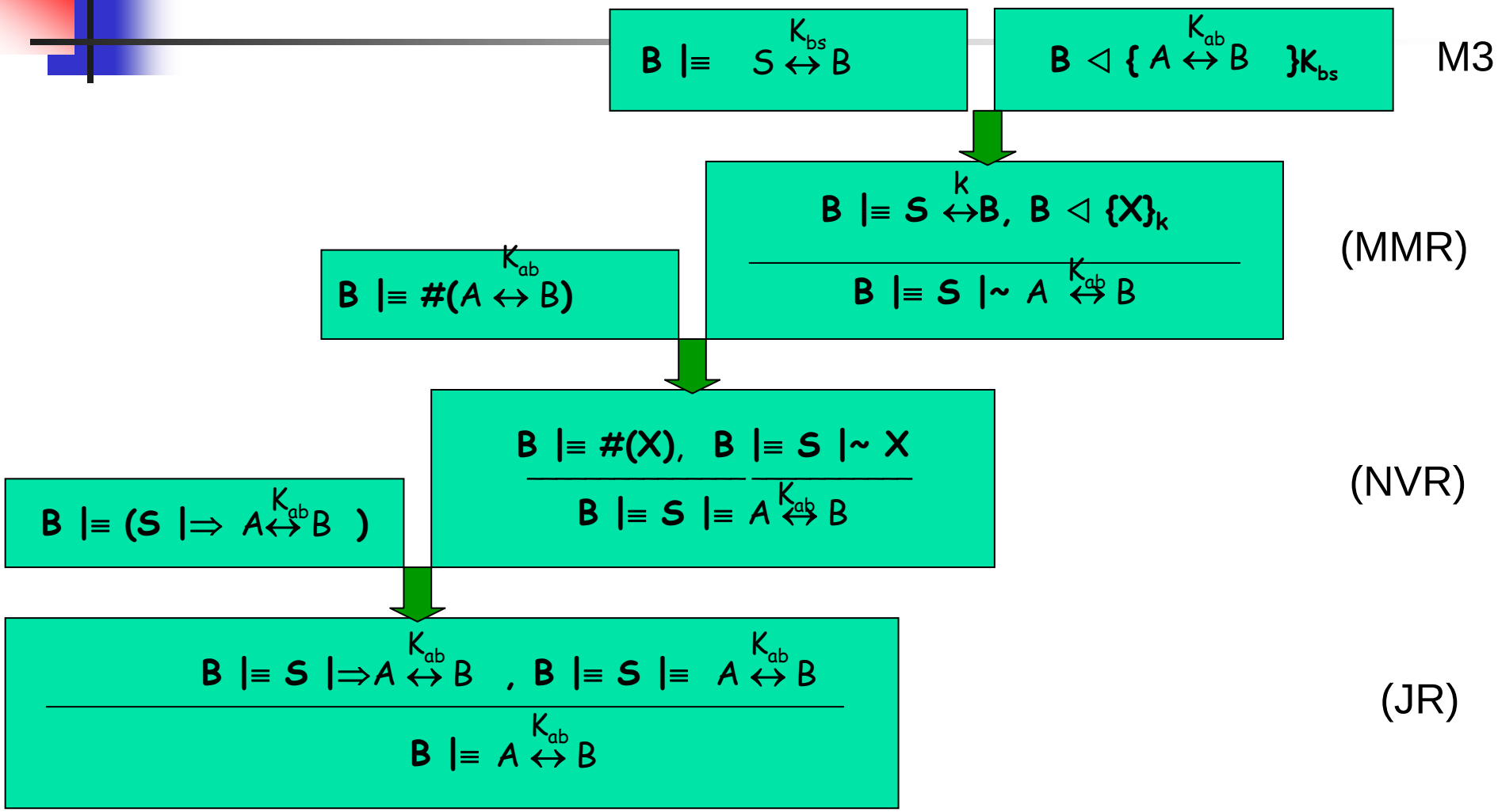
$$A \mid\equiv S \mid\Rightarrow \#(A \overset{K_{ab}}{\leftrightarrow} B)$$

$$\frac{A \mid\equiv S \mid\Rightarrow X,\quad A \mid\equiv S \mid\equiv X}{A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B,}$$

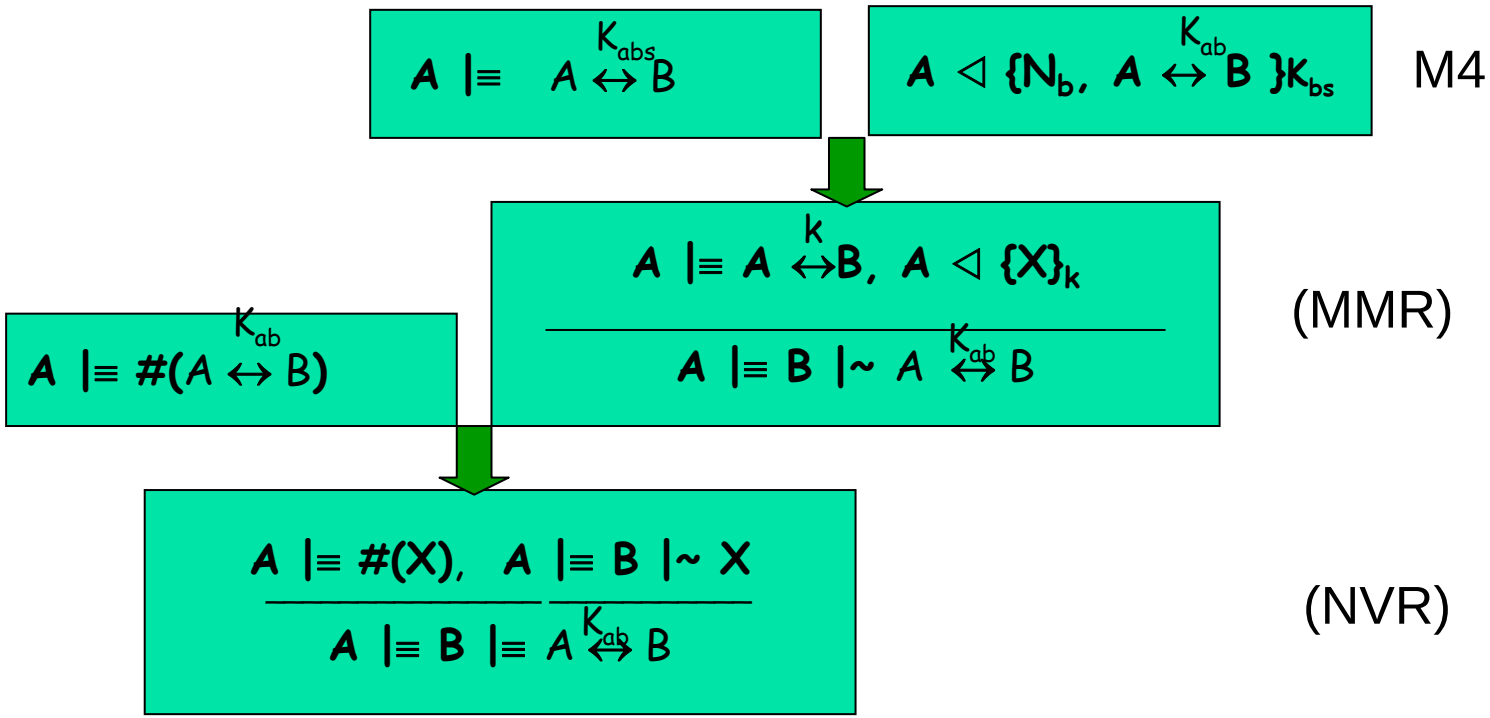
$$\frac{A \mid\equiv S \mid\Rightarrow \#(X),\quad A \mid\equiv S \mid\equiv \#(X)}{A \mid\equiv \#(A \overset{K_{ab}}{\leftrightarrow} B),}$$

(JR)

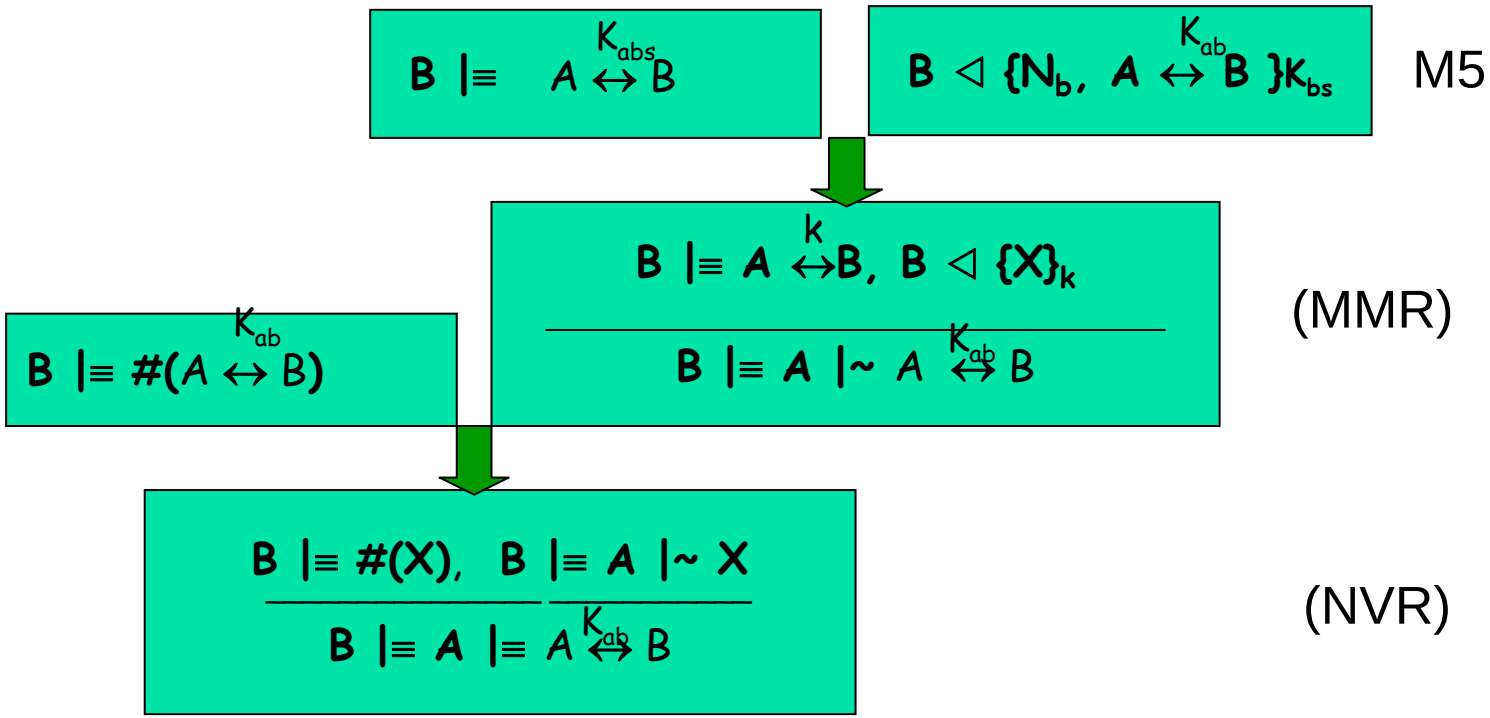
NSSK Verification (Cont'd)



NSSK Verification (Cont'd)



NSSK Verification (Cont'd)



Conclusions of NSSK

We have achieved this:

1. A and B each believe that they share a secret key Kab
2. Both believe that the other believes a secret key Kab

$$B \mid\equiv A \overset{K}{\leftrightarrow} B \text{ (msg 3)} \qquad A \mid\equiv A \overset{K}{\leftrightarrow} B \text{ (msg 2)}$$

We also achieve this final goal:

$$A \mid\equiv B \mid\equiv A \overset{K}{\leftrightarrow} B \text{ (msg 4)} \qquad B \mid\equiv A \mid\equiv A \overset{K}{\leftrightarrow} B \text{ (msg 5)}$$

This authentication protocol has an extra assumption, that is, B assumes the key receives from A is fresh. So Needham-Schroeder protocol had this flaw in it.

Denning-Sacco Attack

If an attacker obtains the old session key, then the attacker (Ã) can impersonate A and the protocol runs as follows:

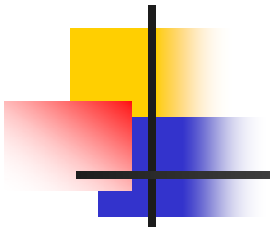
Message 1 $\tilde{A} \rightarrow S$: A, B, N'_A

Message 2 $S \rightarrow \tilde{A}$: $\{N'_A, B, K'_{AB}, \{K'_{AB}, A\}K_{BS}\}\ K_{AS}$

Message 3 $\tilde{A} \rightarrow B$: $\{K_{AB}, A\}K_{BS}$

Message 4 $B \rightarrow \tilde{A}$: $\{N'_B\}K_{AB}$

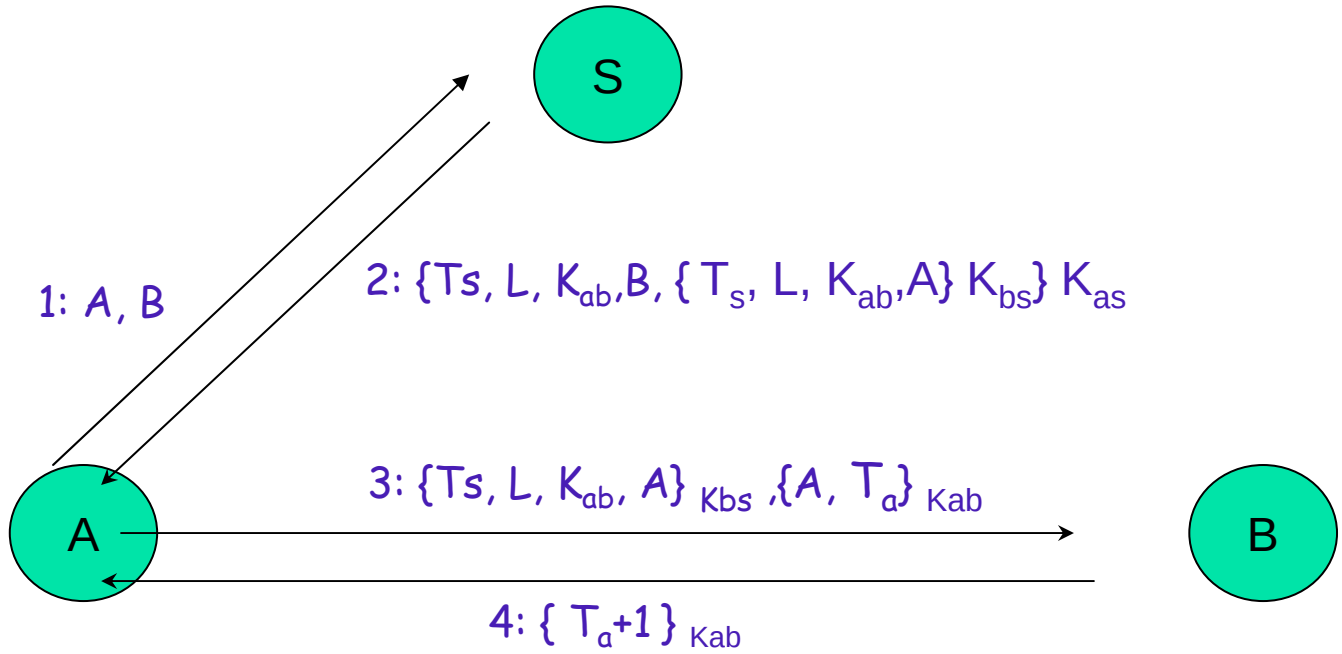
Message 5 $\tilde{A} \rightarrow B$: $\{N'_B - 1\}K_{AB}$



Flaws with BAN Logic

- BAN logic is a belief system and it is different from a knowledge system. Knowledge systems have an axiom of the following form "If you know P, then P is true." However, belief systems do not have this axiom, since a belief in P says nothing about the truth or falsity of P.
- Assumption that all principals taking part in a protocol are honest, in the sense that each principal believes in the truth of each message it sends. However, honesty is not a logical assumption to make.

The Kerberos Protocol



Message1:	$A \rightarrow S$:	A, B
Message2:	$S \rightarrow A$:	$\{Ts, L, K_{ab}, B, \{Ts, L, K_{ab}, A\}_{Kbs}\}_{Kas}$
Message3:	$A \rightarrow B$:	$\{Ts, L, K_{ab}, A\}_{Kbs}, \{A, Ta\}_{Kab}$
Message4:	$B \rightarrow A$:	$\{Ta+1\}_{Kab}$

Idealized protocol

Message1: $A \rightarrow S$: A, B

Message2: $S \rightarrow A$: $\{Ts, L, K_{ab}, B, \{Ts, L, K_{ab}, A\}_{Kbs}\}_{Kbs}$

Message3: $A \rightarrow B$: $\{Ts, L, K_{ab}, A\}_{Kbs}, \{A, Ta\}_{Kab}$

Message4: $B \rightarrow A$: $\{Ta+1\}_{Kab}$

Message2: $S \rightarrow A$: $\{Ts, A \overset{K_{ab}}{\leftrightarrow} B, \{Ts, A \overset{K_{ab}}{\leftrightarrow} B\}_{Kbs}\}_{Kas}$

Message3: $A \rightarrow B$: $\{Ts, A \overset{K_{ab}}{\leftrightarrow} B\}_{Kbs}, \{Ta, A \overset{K_{ab}}{\leftrightarrow} B\}_{Kab}$ from A

Message4: $B \rightarrow A$: $\{Ta, A \overset{K_{ab}}{\leftrightarrow} B\}_{Kab}$ from B

Confusion

Protocol Analysis

- Initial assumptions :

$A \mid\equiv A \overset{K_{as}}{\leftrightarrow} S$

$B \mid\equiv B \overset{K_{bs}}{\leftrightarrow} S$

$S \mid\equiv A \overset{K_{as}}{\leftrightarrow} S$

$S \mid\equiv B \overset{K_{bs}}{\leftrightarrow} S$

$S \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$

$A \mid\equiv (S \mid\Rightarrow A \overset{K_{ab}}{\leftrightarrow} B)$

$B \mid\equiv (S \mid\Rightarrow A \overset{K_{ab}}{\leftrightarrow} B)$

$A \mid\equiv \#(T_a)$

$B \mid\equiv \#(T_s)$

$A \mid\equiv \#(T_s)$

$B \mid\equiv \#(T_a)$

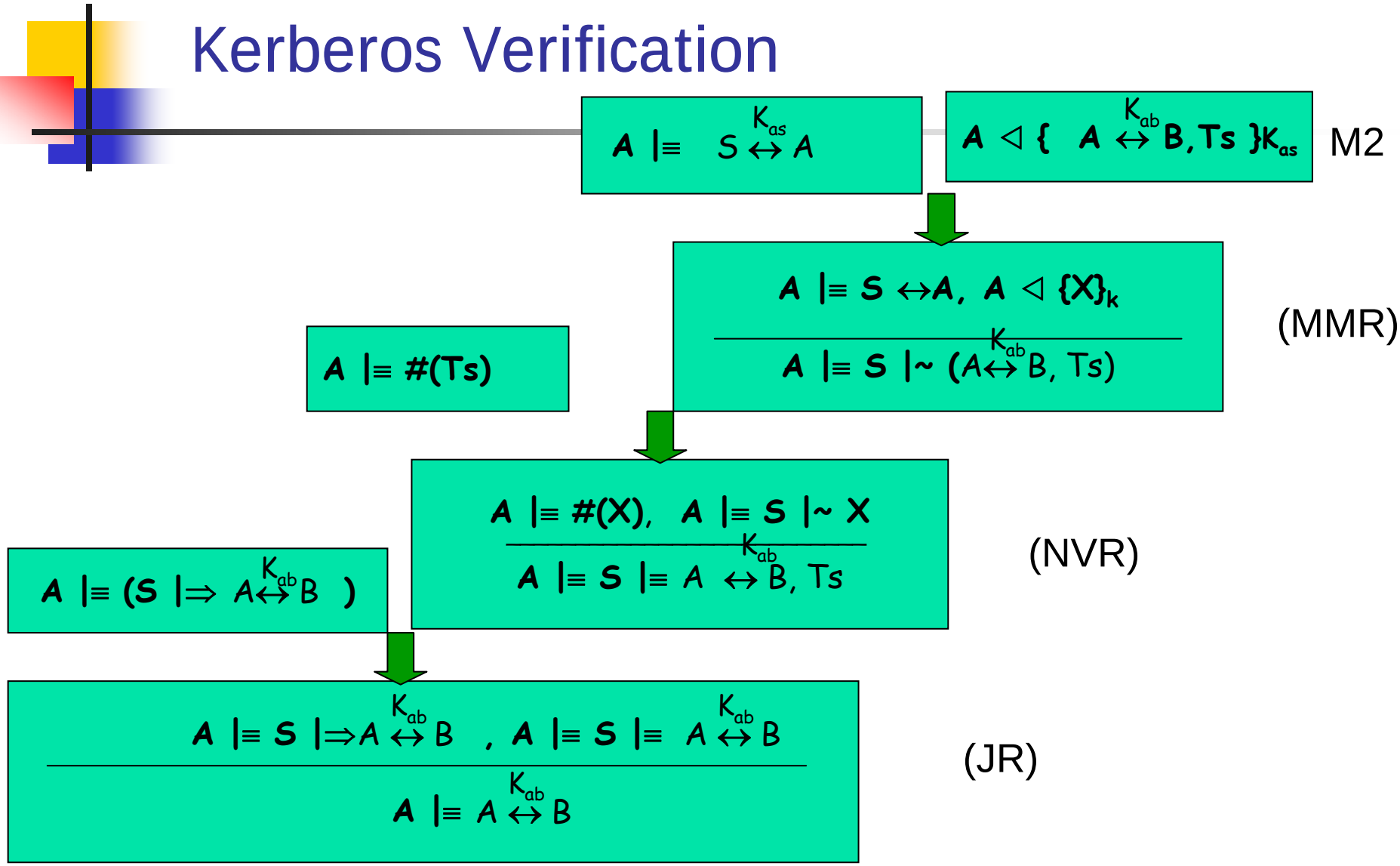
Goal of Authentication

- Prove from the postulate of BAN logic and assumptions, the goal of the protocol is

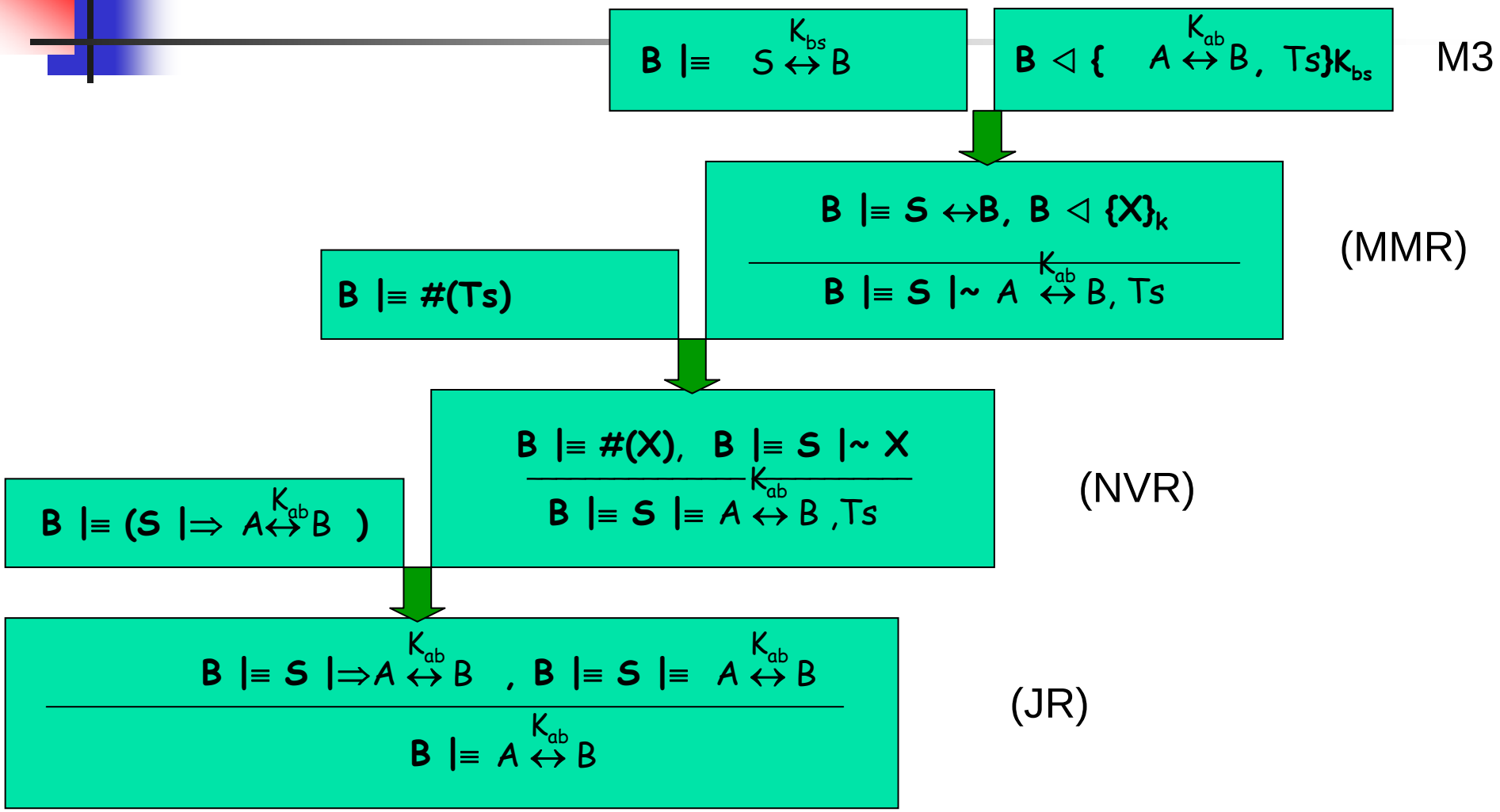
$$A \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

$$B \mid\equiv A \overset{K_{ab}}{\leftrightarrow} B$$

Kerberos Verification



Kerberos Verification (Cont'd)



Needham-Schroeder Public key Protocol (NSPK)

Message 1 $A \rightarrow B$: $\{A, N_a\}K_b$

Message 2 $B \rightarrow A$: $\{N_a, N_b\}\ K_a$

Message 3 $A \rightarrow B$: $\{N_b\}K_b$

NSPK：Idealized Protocol

Corresponding idealized protocol is as follows:

Message 1 $A \rightarrow B$: $\{N_a\} K_b$

Message 2 $B \rightarrow A$: $\overset{N_b}{\{A \leftrightarrow B, N_a\}K_a}$

Message 3 $A \rightarrow B$: $\{ A \overset{N_a}{\leftrightarrow} B, \ B \overset{N_b}{\mid\equiv} A \leftrightarrow B\}K_b$

NSPK : Initial Assumption

$$A \mid\equiv \overset{Ka}{\mapsto} A \qquad B \mid\equiv \overset{Kb}{\mapsto} B$$

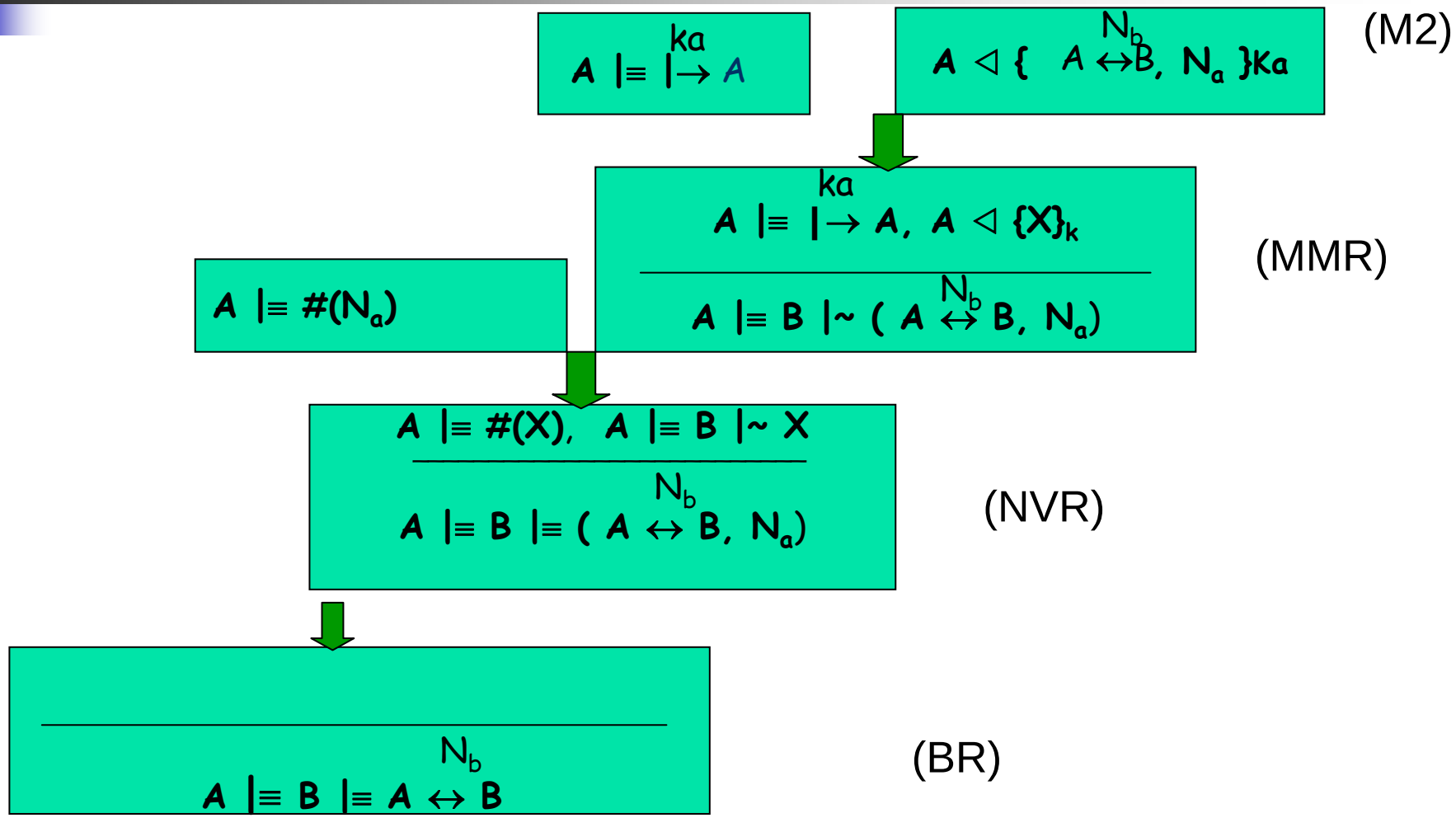
$$A \mid\equiv \#(N_a) \qquad B \mid\equiv \#(N_a)$$

$$A \mid\equiv A \overset{N_a}{\leftrightarrow} B \qquad B \mid\equiv A \overset{N_b}{\leftrightarrow} B$$

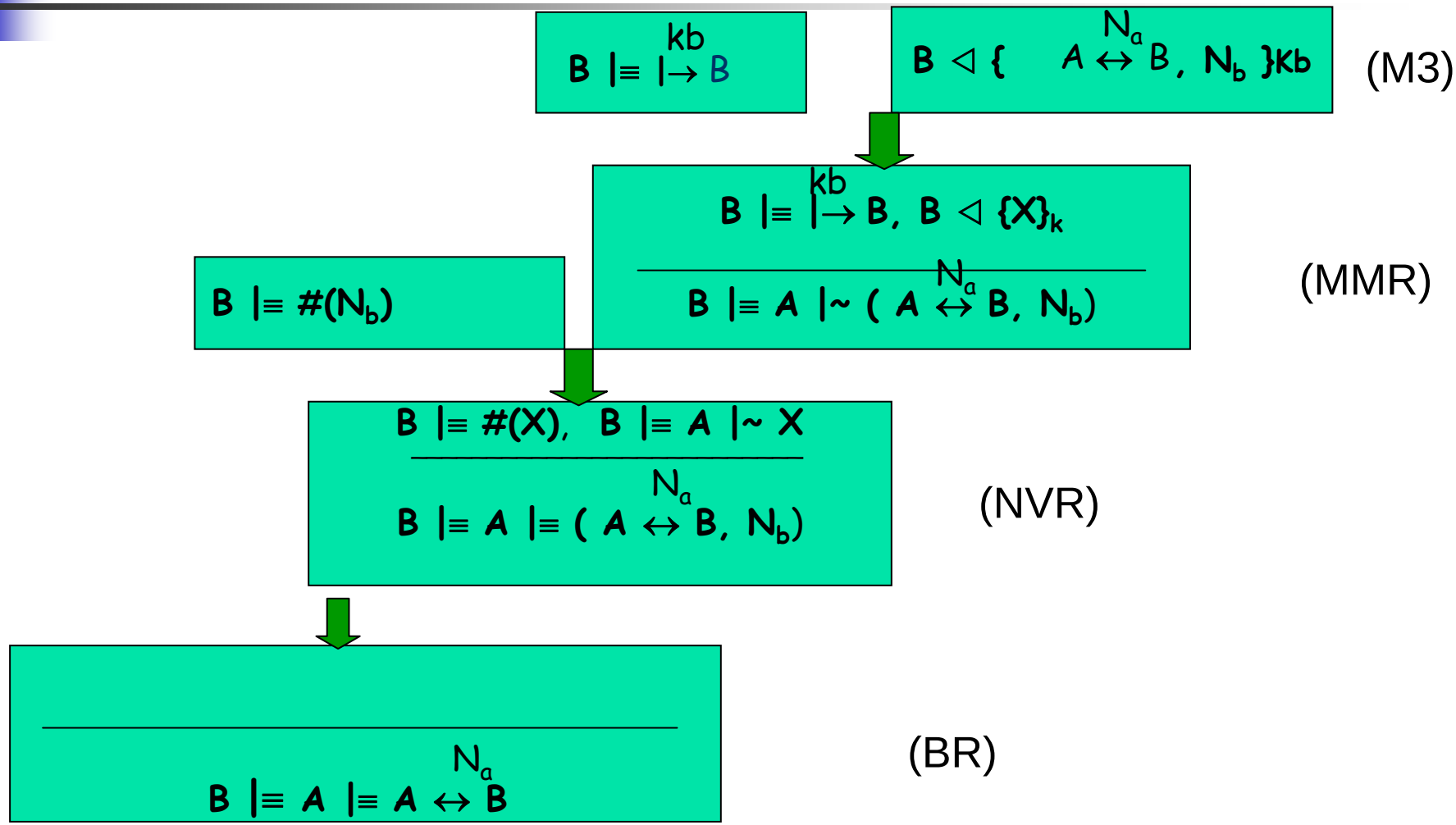
Goals :

$$A \mid\equiv B \mid\equiv A \overset{N_b}{\leftrightarrow} B \qquad B \mid\equiv A \mid\equiv A \overset{N_a}{\leftrightarrow} B$$

NSPK Verification I



NSPK Verification II



Interleaving Attack on NSPK

Message 1 $A \rightarrow E$: $\{A, N_a\}Ke$

i $E_A \rightarrow B$: $\{A, N_a\}Kb$

ii $B \rightarrow E_A$: $\{N_a, N_b\}Ka$

Message 2 $E \rightarrow A$: $\{N_a, N_b\}Ka$

Message 3 $A \rightarrow E$: $\{N_b\}Ke$

iii $E_A \rightarrow B$: $\{N_b\}Kb$

Overcome the Interleaving Attacks

Message 1 $A \rightarrow B$: $\{A, N_a\}K_b$

Message 2 $B \rightarrow A$: $\{N_a, N_b, B\}\ K_a$

Message 3 $A \rightarrow B$: $\{N_b\}K_b$

Preventing the Interleaving Attack on NSPK

Message 1 $A \rightarrow E$: $\{A, N_a\}Ke$

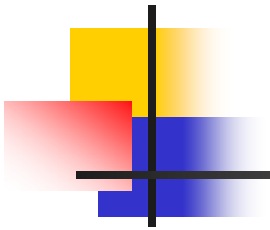
i $E_A \rightarrow B$: $\{A, N_a\}Kb$

ii $B \rightarrow E_A$: $\{N_a, N_b, B\}Ka$

Message 2 $E \rightarrow A$: $\{N_a, N_b, B\}Ka$ (fail and stop!)

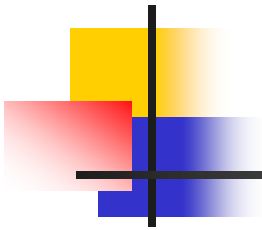
Message 3 $A \rightarrow E$: $\{N_b\}Ke$

iii $E \rightarrow B$: $\{N_b\}Kb$



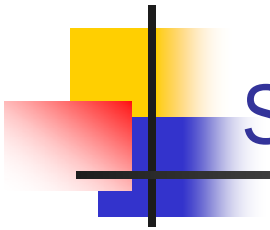
Advantages of BAN Logic

- Huge success for formal methods in cryptography, useful tool
- BAN Logic successful in uncovering implicit assumptions and weaknesses in a number of protocols
- Vehicle for extensive research in the areas for basis and development of other logic systems
- BAN's strengths lie in its simplicity of its logic and its ease of use



Conclusion

- BAN Logic is one of earliest successful attempts at formal reasoning about authentication protocols
- BAN logic involves idealizing a protocol, identifying initial assumptions, using logical postulates to deduce new predicates and determining if the goals of authentication have been met
- BAN logic can be used to analyze existing protocols and detect their flaws
- In the Needham Schroeder protocol, BAN logic helped to uncover an extra assumption that the authors themselves did not realize
- BAN logic has its flaws, but overall it is a welcome success for formal methods in cryptography



Some other approaches

- **Variants of BAN** such as GNY and SVO were invented to address shortcomings of BAN (eg, removing honesty assumption, removing of idealized formalization) and extend the scope.
- **The NRL analyser** treats protocol steps as conditional rewriting rules, and uses search in Prolog to find unreachable states (corresponding to failure of secrecy properties).
- **Process calculi** form a natural setting for describing security protocols, closer to implementations than BAN.
- **The inductive approach** of Paulson formalizes traces as inductively generated from a set of rules, within the higher-order logic of his Isebelle theorem prover.